For the first three $t=1$; for the fourth $t=0, 1$; for the others $t=0$. Of the 17 resulting values of λ, 114, 222, 249, 289, 397, 424, 492 are excluded by mod. 7; then 127, 154, 199, 204, 447 are excluded by mod. 11; 262 and 357 by mod. 13; 87 and 442 by mod. 17; for the remaining value $\lambda=384$, $S\equiv 21$ (mod. 23), whereas 21 is a quadratic non-residue of 23.

Hence $b=\frac{1}{55}(56^7-1)$ *is a prime.*

While it is believed that the above work is accurate, having been carefully checked, it should be added that the same result was found by an earlier proof different as to details.

5. By the same method, I obtain the following results:

$$56^7+1=3.19.15737.1925393,$$
$$34^{17}+1=5.7.307.443.1531.28051.112643.4708729,$$
$$52^{13}+1=53.4057.21841.4328028093013,$$

all of the given factors being prime. That the last number of 13 digits is prime, I have verified by two proofs differing as to details. The factor 21841 was found by accident by Lt. Col. Cunningham. I ran across the factor 112643 of the second number in the manner explained in the *Quarterly Journal*, 1908, page 45; but the remaining two large factors were found by the present method.

6. In view of the interest in the numbers m^m-1 and their importance in connection with the last theorem of Fermat, it is desirable that some arithmetician should check the statement of E. Lucas (*American Journal of Mathematics*, Vol. 1, 1878, p. 294) that the large factors of 10 and 12 digits in $22^{11}\pm 1$ are actually primes. For a verification by the present method it is of the greatest help to know that there are no factors less than 10,000, in view of the tables by Lt. Col. Cunningham. The latter believes that Lucas intended to record his factors as primes; but that an uncertainty runs right through his factorizations as to the primality of the factors, no clue whatever being given as to how the primality was detected.

FACTORING IN A DOMAIN OF RATIONALITY.

By ELIZABETH R. BENNETT, The Universtty of Illinois.

If a series of symbols R_1, R_2, ... which are supposed to obey the ordinary laws of algebra, but are not necessarily thought of as representing numbers, are combined with respect to the four fundamental operations of arithmetic—addition, subtraction, multiplication, and division, division by zero being excluded, there result a series of expressions which are rational with respect to these symbols. The totality of such expressions is called a domain of rationality and it is the smallest possible domain involving the symbols R_1, R_2, ...

If only one of these symbols as R_1 is involved in the combinations and if R_1 is a rational number different from zero, the domain of rational numbers including zero, positive and negative integers, and positive and negative rational fractions is obtained. This domain of rational numbers is included in every domain. The complex numbers of form $a+bi$, where a and b are rational numbers and $i=\sqrt{-1}$, also constitute a domain of rationality which includes the domain of rational numbers.

When we add or adjoin to a known domain a number β which does not already belong to it, the new set of numbers constitutes a domain, if we also add to it all numbers obtained from additions, subtractions, multiplications, and divisions involving β and all numbers of the original domain. The domain of the ordinary complex numbers already mentioned may be formed by the adjunction of i to the domain of rational numbers.

An algebraic integer is a root of the equation

$$x^n+a_1x^{n-1}+a_2x^{n-2}...+a_n=0$$

where a_1, a_2, ..., a_n are rational integers. An algebraic quadratic integer is a root of the above equation when $n=2$. All algebraic quadratic integers are of the form $x+y\sqrt{m}$ when $m\equiv2$ or 3 (mod. 4), and of the form $x+y\,\frac{1+\sqrt{m}}{2}$ when $m\equiv1$ (mod. 4). It is assumed that m is not divisible by any square greater than 1 and that x and y are integral.

The term integral domain is understood, as usual, to mean a set of integral elements which is invariant with respect to addition, subtraction, and multiplication; that is, any combinations of the numbers of the set by the operations mentioned yield again a number belonging to the set. An integral algebraic domain is then an integral domain formed by the adjunction of an algebraic integer to the ordinary integral domain.

In the ordinary integral domain the theorem that a number can be resolved into its positive prime factors in only one way is fundamental. That the above theorem is not valid in all domains is well known and may be easily shown by an example. For instance, $6=2\times3=(1+\sqrt{-5})\,(1-\sqrt{-5})$, the factors of each product being primes in the domain considered. It was in order to avoid such possibilities in factoring, as indicated by the above example, that the theory of ideals was created.

It is also generally known that numbers prime in one domain may be composite in another. For example, in the ordinary integral complex domain every rational prime of the form $4n+3$ is a complex prime and every rational prime of the form $4n+1$ is composite.

In the *Nouvelles Annales de Mathematiques* for 1903, M. G. Fontené has considered algebraic integers of the form $x+y\sqrt{-5}$. In this article it is shown that factoring in the domain of the numbers $x+y\sqrt{-5}$ is not unique, but if the domain is enlarged so as to contain numbers of the form $\frac{x+y\sqrt{-5}}{\sqrt{2}}$ factoring becomes a unique process.

The relation which exists between factoring in a quadratic complex domain and the number of classes of quadratic forms corresponding to the domain has been considered by A. E. Westun in "Certain Systems of Quadratic Complex Numbers," *Transactions of the Cambridge Philosophical Society*, Vol. XVII, 1899. In both of the articles mentioned, factoring is not restricted to operations in an integral quadratic domain.

From the previous definitions and illustrations which are quite generally known, it is evident that an integral algebraic domain can be found by the adjunction of $\sqrt{-6}$ to the ordinary integral domain. This integral algebraic domain will be denoted for brevity by the letter Ω, and some of the properties of numbers in the domain will be considered with special reference to factoring.

We now prove the following theorem:

THEOREM I. *All ordinary primes of the form* $24z+1$ *and* $24z+7$ *are composite in* Ω.

From the theory for binary quadratic forms, it is known that D, the determinant of the form, must be a quadratic residue of m, where m is the number to be represented by the form. The number -6 is a quadratic residue of primes of the form $24z+1$, $24z+7$, $24z+5$, and $24z+11$. There are only two reduced forms for $D=-6$, namely, x^2+6y^2 and $2x^2+3y^2$. The form $2x^2+3y^2$ will not give complex factors in Ω, and so need not be considered. Then all ordinary primes which are composite in Ω must be represented by x^2+6y^2.

If m is the prime to be represented, $m=x^2+6y^2$ and, therefore, $x^2\equiv m$ (mod. 6). $x^2\equiv 1$ (mod. 6), but x^2 is not congruent to 5 (mod. 6) and, therefore, all ordinary primes represented by x^2+6y^2 are of form $24z+1$ and $24z+7$ and only primes of these forms can be factored in Ω.

$$(1-\sqrt{-6})(1+\sqrt{-6})=7; \quad (5-\sqrt{-6})(5+\sqrt{-6})=31.$$

THEOREM II. *Primes of the form* $24z+1$ and $24z+7$ *can be resolved into their complex prime factors in only one way in* Ω.

There are four representations of x^2+6y^2 which give the same prime m. There are two solutions of the congruence $n^2\equiv -6$ (mod. m), and two substitutions transforming x^2+6y^2 into an equivalent form. Therefore, a prime number can be represented by x^2+6y^2 in only one way and consequently primes of the form $24z+1$ and $24z+7$ can be resolved into prime complex factors in only one way in Ω.

THEOREM III. *In order that a composite rational integer may be resolved into complex factors only in* Ω, *it must be of the form,* $m=a^{(\alpha)}b^{(\beta)}c^{\gamma}\,d^{\delta}$, *where a represents primes of the form* $24z+1$ *and* $24z+7$, *and* (α) *the number of primes in a; b represents primes of the form* $24z+5$ *and* $24z+11$ *and* (β) *the number of primes in b;* $c=2$, $d=3$, $(\beta)+\gamma+\delta$ *is an even number and* $\gamma+\delta \not> (\beta)$.

The determinant of this form, that is, -6, must be a quadratic residue of any composite number m properly represented by x^2+6y^2 and, therefore, must be a quadratic residue of every prime factor of m. $x^2+6y^2=m$, or m must be a quadratic residue of 6. The number -6 is a quadratic residue of primes of the form $24z+1$, $24z+7$, $24z+5$, and $24z+11$. Primes of form $24z+1$ and $24z+7$ are quadratic residues of 6, while primes of the form $24z+5$ and $24z+11$ are non-quadratic resides of 6. Then any number $m=a^{(\alpha)}b^{(\beta)}$ is properly representable by x^2+6y^2, or may be resolved into complex factors only in Ω, (β) being even, since an even number of non-quadratic residues is a quadratic residue. We have the following equations:

(I). $2x^2+3y^2=(x\sqrt{2}+y\sqrt{-3})(x\sqrt{2}-y\sqrt{-3})$.

(II). Then $2(2x^2+3y^2)=\sqrt{2}(x\sqrt{2}+y\sqrt{-3}).\sqrt{2}(x\sqrt{2}-y\sqrt{-3})$
$=(2x+y\sqrt{-6})(2x-y\sqrt{-6})=(z+y\sqrt{-6})(z-y\sqrt{-6})$.

(III). Also, $3(2x^2+3y^2)=\sqrt{3}(y\sqrt{3}+x\sqrt{-2}).\sqrt{3}(y\sqrt{3}-x\sqrt{-2})$
$=(3y+x\sqrt{-6})(3y-x\sqrt{-6})=(z'+x\sqrt{-6})(z'-x\sqrt{-6})$.

The primes 2 and 3 are not represented by x^2+6y^2 and are not properly represented by $2x^2+3y^2$. Equations (II) and (III) then show that neither 2^{γ}, 3^{δ}, nor $2^{\gamma}3^{\delta}$ are properly represented, or have complex factors in the domain Ω. Primes of the form $24z+5$ and $24z+11$, however, are properly represented by $2x^2+3y^2$ and an inspection of equations (II) and (III) will show that the product of any such prime b by either 2 or 3 will give a number having complex factors in Ω. Since neither 2^{γ}, 3^{δ} nor $2^{\gamma}3^{\delta}$ have complex factors in Ω, but $2b$ and $3b$ have such factors, $\gamma+\delta$ cannot be greater than (β), $(\beta)-\gamma+\delta$ must be even since all primes of form $24z+5$ and $24z+11$ are non-quadratic residues, (mod. 6). Therefore, $(\beta)+\gamma+\delta$ must be an even number.

THEOREM IV. *Any composite rational integer* $m=a^{(\alpha)}b^{(\beta)}c^{\gamma}\,d^{\delta}$ *representable by the form* x^2+6y^2 *can be resolved into its prime complex factors in more than one way provided it contains at least two different prime factors of the form* $24z+5$ and $24z+11$, *so that* $(\beta)-(\gamma+\delta)\not<\alpha$.

Let Kx represent the composite rational integer, x representing the product of prime factors of form $24z+5$ and $24z+11$, K the product of all other prime factors. K can be resolved into its complex prime factors in only one way because primes of form $24z+1$ and $24z+7$ are resolvable into complex factors in only one way and 2^γ, 3^δ, or $2^\gamma 3^\delta$ have no complex factors in the domain. It is also evident from the previous theorems that no prime of the form $24z+1$ and $24z+7$ combined with either 2 or 3 or with a single prime of the form $24z+5$ or $24z+11$ can be resolved into complex factors only in Ω. $2b$ and $3b$, where b is any prime of form $24z+5$ and $24z+11$, can be resolved into complex factors in only one way since 2 and 3 have no complex factors in Ω. From these statements, it is clear that the factoring in different distinct ways must depend only on the factors of x.

A number x can be represented or resolved into its complex factors in Ω in 2^{w-1} ways where w represents the number of different prime factors of x. These $w-1$ representations will be distinct, since primes of form $24z+5$ and $24z+11$ are also primes in the domain Ω.

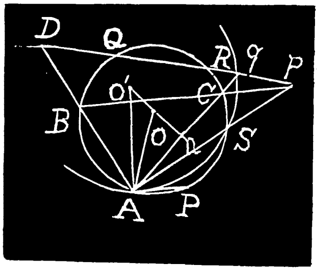
NOTE ON THE STEINER POINT.

By W. GALLATLY, Swanage, England.

Let ABC be the mid-point triangle, and PQR the pedal triangle of a given triangle $A'B'C'$, so that AP is parallel to BC, and $AQ=AR=BC=a$: $(a>b>c)$. And since rq is antiparallel to BC, $\angle Arq=C$, $\angle Aqr=B$.

Describe a circle around $\triangle Aqr$. This touches AP since $\angle Arq=C=\angle CAP$, and therefore the center O' lies on the perpendicular from A on BC. Join Ap, cutting the circle ABC in S. Then S is the Steiner point of the triangle ABC.

Since q, C, B, r are cyclic, $pq.pr=pC.pB=pS.pA$. Hence S lies on the circle Aqr. To find the radius, ρ, of this circle, we have $Aq=2\rho.\sin Arq$ $=2\rho.\sin C$. Also $Aq=AR.\dfrac{\sin A}{\sin B}=2R\sin A.\dfrac{\sin A}{\sin B}$, where R is the radius of the circle ABC. Therefore $\rho=R.\dfrac{a^2}{b^2}$.



To determine the length of AS.

In the triangle OAO', $OA=R$, $O'A=R.a^2/bc$, $\angle OAO'=\angle B-\angle C$, and $OO'^2=OA^2+O'A^2-2.OA.O'A.\cos\angle OAO'$.

But $\cos B\cos C=\dfrac{a^4-(b^2-c^2)^2}{4a^2bc}$, $\sin B\sin C=\dfrac{16\triangle^2}{4a^2bc}$, where $\triangle^2$ is the square of the area of the triangle ABC.

Hence, $\dfrac{OO'^2}{R^2}.b^2c^2=a^4+\ldots-b^2c^2-\ldots=\dfrac{a^2b^2c^2.e^2}{4R^2\sin^2\omega}$, where e is the eccentricity of the Brocard ellipse, and ω is the Brocard angle.